On Complementarity In QEC And Quantum Cryptography

David Kribs

Professor & Chair
Department of Mathematics & Statistics
University of Guelph

Associate Member
Institute for Quantum Computing
University of Waterloo

QEC II — USC — December 2011

Outline

Notation

- $\mathcal{H}_A$, $\mathcal{H}_B$ will denote Hilbert spaces for systems A and B.
- $\mathcal{B}(\mathcal{H})$ will denote the set of (bounded) linear operators on $\mathcal{H}$; $\mathcal{B}(\mathcal{H})_t$ will denote the trace class operators on $\mathcal{H}$. In finite dimensions these sets coincide and so we'll simply write $\mathcal{L}(\mathcal{H})$
- $\mathcal{B}(\mathcal{H}_A, \mathcal{H}_B)$ will denote the set of linear transformations from $\mathcal{H}_A$ to $\mathcal{H}_B$.
- We'll write X, Y for operators in $\mathcal{B}(\mathcal{H})$, and ρ, σ for density operators in $\mathcal{B}(\mathcal{H})_t$. (And we'll just refer to $\mathcal{L}(\mathcal{H})$ when appropriate.)
- Given a linear map $\Phi : \mathcal{B}(\mathcal{H}_A)_t \to \mathcal{B}(\mathcal{H}_B)_t$, its dual map $\Phi^\dagger : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_A)$ is defined via the Hilbert-Schmidt inner product: $\mathrm{Tr}(\rho\, \Phi^\dagger(X)) = \mathrm{Tr}(\Phi(\rho)X)$.

Heisenberg Picture

- Suppose that $\Phi^\dagger : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_A)$ is a completely positive (CP) unital ($\Phi^\dagger(I_B) = I_A$) linear map.

Heisenberg Picture

- Suppose that $\Phi^\dagger : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_A)$ is a completely positive (CP) unital ($\Phi^\dagger(I_B) = I_A$) linear map.
- Then there is a Hilbert space $\mathcal{K}$ (of dimension at most $\dim(A)\dim(B)$) and a co-isometry $V \in \mathcal{B}(\mathcal{H}_B \otimes \mathcal{K}, \mathcal{H}_A)$ ($VV^\dagger = I_A$) such that

$$\Phi^\dagger(X) = V(X \otimes I_\mathcal{K})V^\dagger \qquad \forall X.$$

Heisenberg Picture

- Suppose that $\Phi^\dagger : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_A)$ is a completely positive (CP) unital ($\Phi^\dagger(I_B) = I_A$) linear map.
- Then there is a Hilbert space $\mathcal{K}$ (of dimension at most $\dim(A)\dim(B)$) and a co-isometry $V \in \mathcal{B}(\mathcal{H}_B \otimes \mathcal{K}, \mathcal{H}_A)$ ($VV^\dagger = I_A$) such that

$$\Phi^\dagger(X) = V(X \otimes I_\mathcal{K})V^\dagger \qquad \forall X.$$

- V is unique up to a unitary on $\mathcal{K}$. Here the Kraus operators for $\Phi^\dagger$ can be read off as the "coordinate operators" of $V^\dagger$:

$$V^\dagger = \begin{bmatrix} V_1^\dagger \\ \vdots \\ V_{AB}^\dagger \end{bmatrix}$$

Schrödinger Picture

- Suppose that $\Phi : \mathcal{B}(\mathcal{H}_A)_t \rightarrow \mathcal{B}(\mathcal{H}_B)_t$ is a CP trace preserving (CPTP) linear map.

Schrödinger Picture

- Suppose that $\Phi : \mathcal{B}(\mathcal{H}_A)_t \to \mathcal{B}(\mathcal{H}_B)_t$ is a CP trace preserving (CPTP) linear map.
- Then there is a Hilbert space $\mathcal{K}$ (of dimension at most $\dim(A)\dim(B)$), an isometry $U \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{K}, \mathcal{H}_B \otimes \mathcal{K})$, and a pure state $|\psi\rangle \in \mathcal{K}$ such that

$$\Phi(\rho) = \mathrm{Tr}_{\mathcal{K}}(U(\rho \otimes |\psi\rangle\langle\psi|)U^\dagger) \qquad \forall \rho.$$

Schrödinger Picture

- Suppose that $\Phi : \mathcal{B}(\mathcal{H}_A)_t \to \mathcal{B}(\mathcal{H}_B)_t$ is a CP trace preserving (CPTP) linear map.
- Then there is a Hilbert space $\mathcal{K}$ (of dimension at most $\dim(A)\dim(B)$), an isometry $U \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{K}, \mathcal{H}_B \otimes \mathcal{K})$, and a pure state $|\psi\rangle \in \mathcal{K}$ such that

$$\Phi(\rho) = \mathrm{Tr}_{\mathcal{K}}(U(\rho \otimes |\psi\rangle\langle\psi|)U^\dagger) \qquad \forall \rho.$$

- The two pictures are connected via $V^\dagger|\phi\rangle := U(|\phi\rangle \otimes |\psi\rangle)$, which gives $\Phi(\rho) = \mathrm{Tr}_{\mathcal{K}}(V^\dagger \rho V)$.

Schrödinger Picture

- Suppose that $\Phi : \mathcal{B}(\mathcal{H}_A)_t \to \mathcal{B}(\mathcal{H}_B)_t$ is a CP trace preserving (CPTP) linear map.
- Then there is a Hilbert space $\mathcal{K}$ (of dimension at most $\dim(A)\dim(B)$), an isometry $U \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{K}, \mathcal{H}_B \otimes \mathcal{K})$, and a pure state $|\psi\rangle \in \mathcal{K}$ such that

$$\Phi(\rho) = \mathrm{Tr}_{\mathcal{K}}(U(\rho \otimes |\psi\rangle\langle\psi|)U^\dagger) \qquad \forall \rho.$$

- The two pictures are connected via $V^\dagger|\phi\rangle := U(|\phi\rangle \otimes |\psi\rangle)$, which gives $\Phi(\rho) = \mathrm{Tr}_{\mathcal{K}}(V^\dagger \rho V)$.
- The Kraus operators for Φ are the coordinate operators V_i from above, and the general form for U is

$$U = \left[V^\dagger \;\middle|\; * \right]$$

Purification of Mixed States

- Fix a density operator $\rho_0 \in \mathcal{B}(\mathcal{H})_t$, and consider the CPTP map $\Phi : \mathbb{C} \to \mathcal{B}(\mathcal{H})_t$ defined by

$$\Phi(c \cdot 1) = c\,\rho_0 \qquad \forall c \in \mathbb{C}.$$

Purification of Mixed States

- Fix a density operator $\rho_0 \in \mathcal{B}(\mathcal{H})_t$, and consider the CPTP map $\Phi : \mathbb{C} \to \mathcal{B}(\mathcal{H})_t$ defined by

$$\Phi(c \cdot 1) = c\,\rho_0 \qquad \forall c \in \mathbb{C}.$$

- Then the Stinespring Theorem gives (here $\mathcal{K} = \mathbb{C} \otimes \mathcal{H} = \mathcal{H}$):

$$\rho_0 = \Phi(1) = \mathrm{Tr}_{\mathcal{K}}(U(1 \otimes |\psi\rangle\langle\psi|)U^\dagger) = \mathrm{Tr}_{\mathcal{K}}(|\psi'\rangle\langle\psi'|),$$

where $|\psi'\rangle \in \mathcal{H} \otimes \mathcal{H}$ is a purification of ρ_0 – and the unitary freedom in the theorem captures all purifications.

Conjugate/Complementary Channels

Definition

(King, et al.; Holevo) Given a CPTP map $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$, *consider* $V \in \mathcal{L}(\mathcal{H}_B \otimes \mathcal{K}, \mathcal{H}_A)$ *and* $\mathcal{K}$ *above for which*

$$\Phi(\rho) = \mathrm{Tr}_{\mathcal{K}}(V^\dagger \rho V).$$

Then the corresponding **conjugate** *(or* **complementary***) channel is the CPTP map* $\widetilde{\Phi} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{K})$ *given by*

$$\widetilde{\Phi}(\rho) = \mathrm{Tr}_{\mathcal{B}}(V^\dagger \rho V).$$

Fact: Any two conjugates $\widetilde{\Phi}$, Φ' obtained in this way are related by a partial isometry W such that $\widetilde{\Phi}(\cdot) = W\Phi'(\cdot)W^\dagger$. We talk of "the" conjugate channel for Φ with this understanding.

Computing Kraus Operators for Conjugates

- Suppose that $V_i \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ are the Kraus operators for $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$. Then we can obtain Kraus operators $\{R_\mu\}$ for $\widetilde{\Phi}$ as follows.

Computing Kraus Operators for Conjugates

- Suppose that $V_i \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ are the Kraus operators for $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$. Then we can obtain Kraus operators $\{R_\mu\}$ for $\widetilde{\Phi}$ as follows.
- Fix a basis $\{|e_i\rangle\}$ for $\mathcal{K}$ and define for $\rho \in \mathcal{L}(\mathcal{H}_A)$,

$$F(\rho) = \sum_{i,j} |e_i\rangle\langle e_j| \otimes V_i \rho V_i^\dagger \in \mathcal{L}(\mathcal{K} \otimes \mathcal{H}_B).$$

Computing Kraus Operators for Conjugates

- Suppose that $V_i \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ are the Kraus operators for $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$. Then we can obtain Kraus operators $\{R_\mu\}$ for $\widetilde{\Phi}$ as follows.
- Fix a basis $\{|e_i\rangle\}$ for $\mathcal{K}$ and define for $\rho \in \mathcal{L}(\mathcal{H}_A)$,

$$F(\rho) = \sum_{i,j} |e_i\rangle\langle e_j| \otimes V_i \rho V_i^\dagger \in \mathcal{L}(\mathcal{K} \otimes \mathcal{H}_B).$$

- Then $\Phi(\rho) = \mathrm{Tr}_{\mathcal{K}} F(\rho)$ and

$$\widetilde{\Phi}(\rho) = \mathrm{Tr}_{\mathcal{B}} F(\rho) = \sum_{i,j} \mathrm{Tr}(V_i \rho V_j^\dagger)|e_i\rangle\langle e_j| = \sum_\mu R_\mu \rho R_\mu^\dagger,$$

where $R_\mu^\dagger = [V_1^\dagger|f_\mu\rangle \; V_2^\dagger|f_\mu\rangle \cdots]$ and $\{|f_\mu\rangle\}$ is a basis for $\mathcal{H}_B$.

Private Quantum Codes

Definition

(Ambainis, et al.) Let $\mathcal{S} \subseteq \mathcal{H}$ be a set of pure states, let $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a CPTP map, and let $\rho_0 \in \mathcal{L}(\mathcal{H})$. Then $[\mathcal{S}, \Phi, \rho_0]$ is a private quantum channel if we have

$$\Phi(|\psi\rangle\langle\psi|) = \rho_0 \quad \forall |\psi\rangle \in \mathcal{S}.$$

Motivating class of examples: random unitary channels, where $\Phi(\rho) = \sum_i p_i U_i \rho U_i^\dagger$.

Single Qubit Private Codes

Recall a single qubit pure state $|\psi\rangle$ can be written

$$|\psi\rangle = \cos\frac{\theta}{2}\begin{pmatrix}1\\0\end{pmatrix} + e^{i\varphi}\sin\frac{\theta}{2}\begin{pmatrix}0\\1\end{pmatrix}.$$

We associate $|\psi\rangle$ with the point (θ, φ), in spherical coordinates, on the Bloch sphere via $\alpha = \cos\left(\frac{\theta}{2}\right)$ and $\beta = e^{i\varphi}\sin\left(\frac{\theta}{2}\right)$. The associated Bloch vector is $\vec{r} = (\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)$. Using the Bloch sphere representation, we can associate to any single qubit density operator ρ a Bloch vector $\vec{r} \in \mathbb{R}^3$ satisfying $\|\vec{r}\| \leq 1$, where

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2}.$$

We use $\vec{\sigma}$ to denote the Pauli vector; that is, $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)^T$.

Single Qubit Private Codes

Every unital qubit channel Φ can be represented as

$$\Phi\left(\frac{1}{2}\left[I+\vec{r}\cdot\vec{\sigma}\right]\right)=\frac{1}{2}\left[I+(T\vec{r})\cdot\vec{\sigma}\right],$$

where T is a 3×3 real matrix that represents a deformation of the Bloch sphere.

We are interested in cases where $\mathcal{S}$ is nonempty. So we consider the cases in which T has non-trivial nullspace; that is, the subspace of vectors $\vec{r}$ such that $T\vec{r}=0$ is one, two, or three-dimensional.

Single Qubit Private Codes

Theorem

Let $\Phi : \mathbb{M}_2 \to \mathbb{M}_2$ be a unital qubit channel, with T the mapping induced by Φ as above. Then there are three possibilities for a private quantum channel $[\mathcal{S}, \Phi, \frac{1}{2}I]$ with $\mathcal{S}$ nonempty:

1. *If the nullspace of T is 1-dimensional, then $\mathcal{S}$ consists of a pair of orthonormal states.*
2. *If the nullspace of T is 2-dimensional, then the set $\mathcal{S}$ is the set of all trace vectors (see below) of the subalgebra $U^\dagger \Delta_2 U$ of 2×2 diagonal matrices up to a unitary equivalence.*
3. *If the nullspace of T is 3-dimensional, then Φ is the completely depolarizing channel and $\mathcal{S}$ is the set of all unit vectors. In other words, $\mathcal{S}$ is the set of all trace vectors of $\mathbb{C} \cdot I_2$.*

Nullspace of T is 1-dimensional

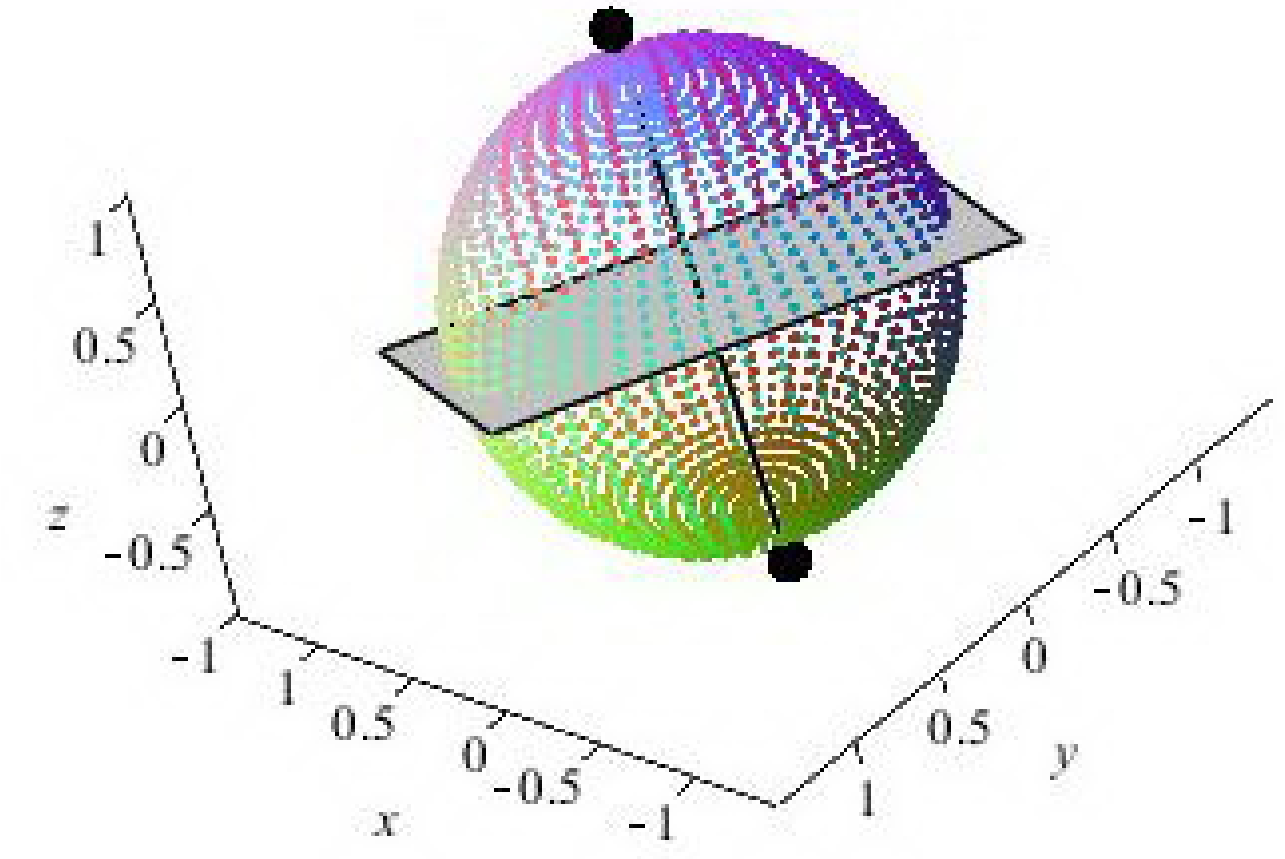

Figure: Case (1)

Nullspace of T is 2-dimensional

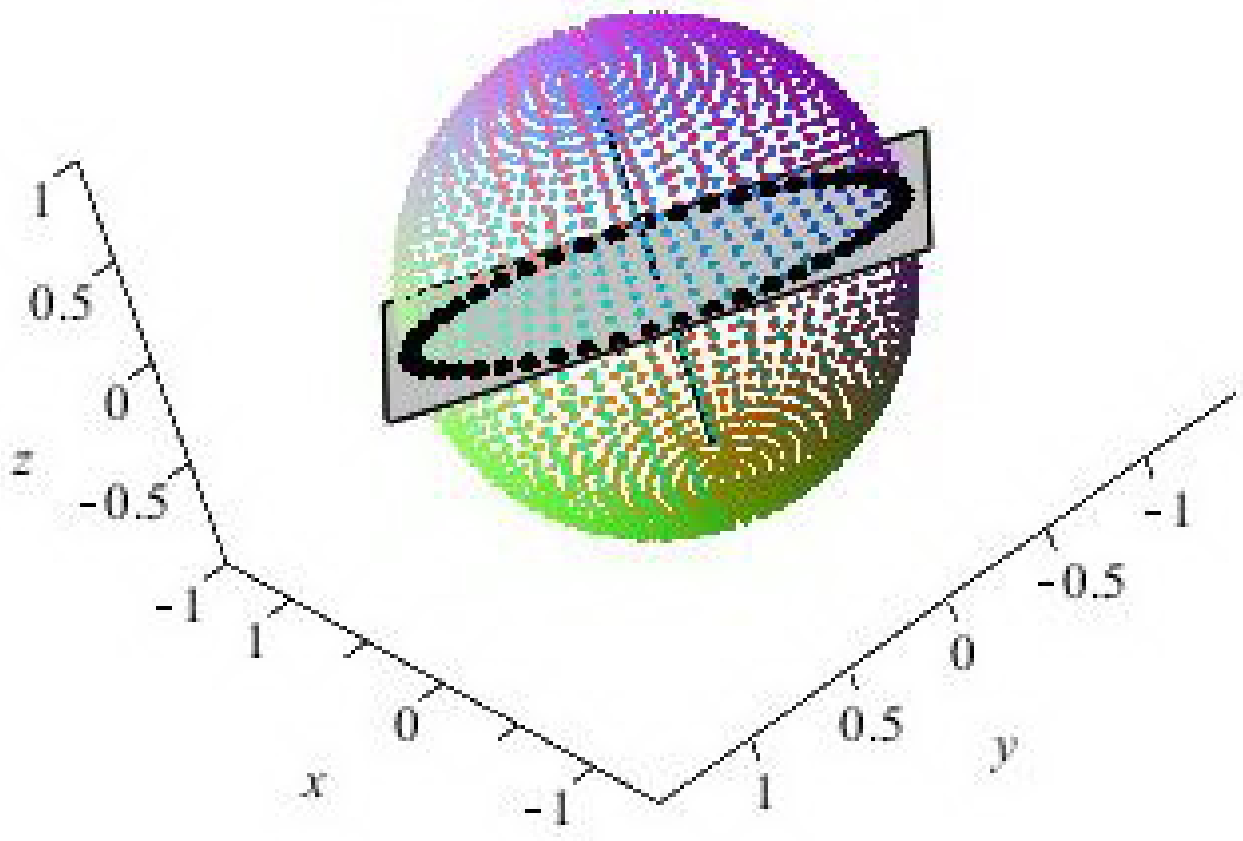

Figure: Case (2)

Nullspace of T is 3-dimensional

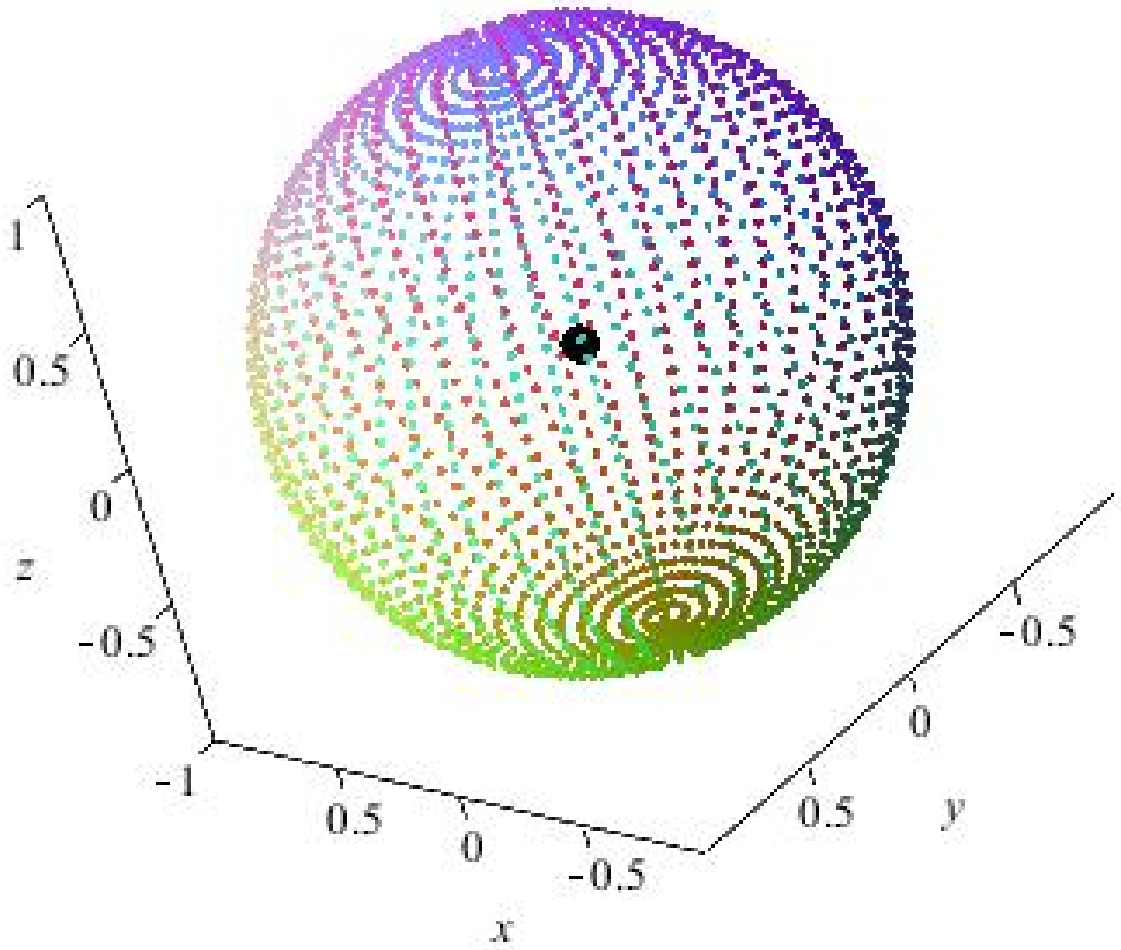

Figure: Case (3)

Private Code Side-Bar

Note: There are interesting connections between private quantum codes and the notions of conditional expectations and trace vectors in the theory of operator algebras – maybe as far back as eighty years ago. For more on this see:

A. Church, D.W. Kribs, R. Pereira, S. Plosker, *Private Quantum Channels, Conditional Expectations, and Trace Vectors*. Quantum Information & Computation, **11** (2011), no. 9 & 10, 774 - 783.

Complementarity of Quantum Codes

Theorem

(Kretschmann-K.-Spekkens) Given a conjugate pair of CPTP maps Φ, $\widetilde{\Phi}$, a code is an error-correcting code for one if and only if it is a private code for the other.

The extreme example of this phenomena is given by a unitary channel paired with the completely depolarizing channel – where the entire Hilbert space is the code.

Example 4.1

- Consider the 2-qubit swap channel $\Phi(\sigma \otimes \rho) = \rho \otimes \sigma$, which has a single Kraus operator, the swap unitary U.
- The conjugate map $\widetilde{\Phi} : \mathcal{L}(\mathbb{C}^2 \otimes \mathbb{C}^2) \to \mathbb{C}$ is implemented with four Kraus operators, which are

$$R_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}$$

$$R_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix}$$

$$R_3 = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}$$

$$R_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix},$$

and one can easily see that $\widetilde{\Phi}(\rho) = 1$ for all $\rho \in \mathcal{L}(\mathbb{C}^2)$.

Example 4.2

Consider the 2-qubit phase flip channel Φ with (equally weighted) Kraus operators $\{I, Z_1\}$. The dilation Hilbert space here is 3-qubits in size, and the conjugate channel $\widetilde{\Phi} : \mathcal{L}(\mathbb{C}^2 \otimes \mathbb{C}^2) \to \mathcal{L}(\mathbb{C}^2)$ is implemented with the following Kraus operators:

$$R_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad R_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$R_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix} \quad R_4 = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Example 4.2

- We have $\Phi(\rho) = \frac{1}{2}(\rho + Z_1\rho Z_1)$ and $\widetilde{\Phi}(\rho) = \sum_{i=1}^{4} R_i \rho R_i^\dagger$ for all 2-qubit ρ.
- It is clear that the code $\{|00\rangle, |01\rangle\}$ is correctable for Φ; in fact it is noiseless/decoherence-free. And thus we know it is private for the conjugate channel $\widetilde{\Phi}$.
- Indeed, one can check directly that every density operator ρ supported on $\{|00\rangle, |01\rangle\}$, satisfies

$$\widetilde{\Phi}(\rho) = |+\rangle\langle+| = \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|).$$

From QEC to QCrypto?

General Program: Using the "algebraic bridge" given by the notion of conjugate channels, investigate what results, techniques, special types of codes, applications, etc, etc, from QEC have analogues or versions in the world of private quantum codes and quantum cryptography. At the least, we can use work from QEC as motivation for studies in this different setting...

"Knill-Laflamme" Type Conditions for Private Codes

Theorem

(K.-Plosker) A projection P is a private code for a CPTP map Φ with output state ρ_0; i.e., $\Phi(\rho) = \rho_0$ for all $\rho \in \mathcal{L}(P\mathcal{H})$

if and only if

$$\forall X \; \exists \lambda_X \in \mathbb{C} \quad : \quad P\Phi^\dagger(X)P = \lambda_X P.$$

In this case, $\lambda_X = \mathrm{Tr}(\rho_0 X)$.

"Knill-Laflamme" Type Conditions for Private Codes

- **QEC Motivation:** If P is correctable for $\widetilde{\Phi}$ then $\exists \lambda_{\mu\nu} \in \mathbb{C}$ such that $PR_\mu^\dagger R_\nu P = \lambda_{\mu\nu} P$. But

$$PR_\mu^\dagger R_\nu P = P\Phi^\dagger(|f_\mu\rangle\langle f_\nu|)P.$$

- **Consequence:** For instance in the case that $\rho_0 \propto Q = \sum_k |\psi_k\rangle\langle\psi_k|$ and $P = \sum_l |\phi_l\rangle\langle\phi_l|$, it follows that there are scalars u_{ikl} such that for all i

$$V_i P = \sum_{k,l} u_{ikl} A_{kl} \quad \text{where} \quad A_{kl} = \frac{1}{\sqrt{rank(Q)}} |\psi_k\rangle\langle\phi_l|.$$

Conclusion

- The Stinespring Dilation Theorem is a foundational mathematical result for quantum information, and it naturally gives rise to the notion of conjugate channels.
- Private quantum codes are a basic tool in quantum cryptography, and can also be viewed from an operator theoretic perspective.
- Quantum error correcting codes are complementary to private quantum codes, with conjugate channels providing a clean algebraic bridge between the two studies.
- It should be possible to develop analogues of many results, techniques, applications, etc, from QEC for use in quantum cryptography. We have discussed some here, but there seem to be many other natural questions...

THANK YOU !